UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/820,673	04/08/2004	James M. Alkove	MSFT-2867/306926.2	8031

41505 7590 05/01/2006

WOODCOCK WASHBURN LLP (MICROSOFT CORPORATION)
ONE LIBERTY PLACE - 46TH FLOOR
PHILADELPHIA, PA 19103

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/820,673	ALKOVE ET AL.	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 April 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *02/01/06 &02/01/20*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-23 are presented for examination.

Drawings

2. Figure 1 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Double Patenting

1. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2. Claims 1-23 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-16 of copending Application No. 10820666. Although the conflicting claims are not identical, they are not patentably distinct from each other because the application '666 teaches all the claims limitation except the differences that are underlined in the following table as an example:

Instant application 10/820673	**Copending application 10/820666**
12. A method of delivering content from a source to a sink by way of a computing device, the method comprising: • an application on the computing device calling to a media base on the computing device with a definition of the content, the source, and the sink; • the media base establishing a protected media path based on the defined content, source, and sink to effectuate such delivery, the established protected media path including: • the media base; • a source trust authority (SOTA) associated with and corresponding to the source, the SOTA acting as a secure lockbox connecting the source to the media base and representing the source in the protected media path, <u>decrypting the content from the source if necessary, and</u>	1. A method of delivering content from a source to a sink by way of a computing device, the method comprising: • an application on the computing device calling to a media base on the computing device with a definition of the content, the source, and the sink; • the media base establishing a protected media path based on the defined content, source, and sink to effectuate such delivery, the established protected media path including: • the media base; • a source trust authority (SOTA) associated with and corresponding to the source, the SOTA acting as a secure lockbox connecting the source to the media base and representing the source in the protected media path; and • a sink trust authority (SITA) associated with and corresponding to the sink, the SITA acting as a secure lockbox connecting the sink to the media base and representing the sink in the protected media

translating policy associated with the content from a native format into a format amenable to the policy engine if necessary; and • a sink trust authority (SITA) associated with and corresponding to the sink, the SITA acting as a secure lockbox connecting the sink to the media base and representing the sink in the protected media path, encrypting content to be delivered to the sink if necessary, and translating the policy associated with the content from the format of the policy engine into a format amenable to the sink if necessary, whereby the sink receives the content and corresponding policy, decrypts the received content if necessary, and renders same based on the received policy; • the SOTA on behalf of the source establishing trust with respect to the protected media path; • the SOTA upon trust being established with respect to the protected media path propagating policy corresponding to the content to be delivered to the protected media path; • the SOTA determining a particular type of action to be taken with the content as delivered through the protected media path; • the SOTA deciding whether	path; • the SOTA on behalf of the source establishing trust with respect to the protected media path; • the SOTA upon trust being established with respect to the protected media path propagating policy corresponding to the content to be delivered to the protected media path; • the SOTA determining a particular type of action to be taken with the content as delivered through the protected media path; • the SOTA deciding with regard to the propagated policy that the particular type of action cannot be taken with the content as delivered through the protected media path and informing the media base of a refusal to take such action; • the media base informing the application of the refusal to take the action; • the SOTA recognizing that the refusal may be rectified by way of a particular enabler available to such SOTA and the SOTA providing the particular enabler to the application by way of the media base, the provided enabler including information and methods necessary for the application to obtain data necessary to respond to the refusal; • the application receiving the enabler at an interface thereof by way of the media base, and the interface applying a common interaction procedure to run the enabler to obtain the data necessary to respond to the refusal; • the application providing the obtained data to the media base

the particular type of action can be taken with the content as delivered through the protected media path and informing the media base regarding same; • the media base informing the application whether the particular type of action can be taken, and if so the application proceeding by commanding the media base to perform such type of action. 19. The method of claim 18 <u>wherein if the policy engine determines that a particular element of the protected media path does not satisfies the policy, the policy engine performs an action selected from a group consisting of refusing such element access to the content and preventing content from being delivered through the protected media path.</u>	and the media base employing the provided data to respond to the refusal; • the SOTA deciding with regard to the propagated policy and based at least in part on the responded refusal that the particular type of action can be taken with the content as delivered through the protected media path and informing the media base regarding same; and • the media base informing the application that the particular type of action can be taken, and the application proceeding by commanding the media base to perform such type of action.

3. This is a <u>provisional</u> obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

4. The differences between these two applications is that the instant application ''673 has a broader claim limitation as underlined above and the copending application has narrower claim limitations and a secure lockbox act of decrypting/encrypting the content from the source if necessary, and translating policy associated with the content from a native format into a format amenable to the policy engine if necessary is not disclosed in '666 of claim limitations. Wherein said action, as described in the disclosure of the instant application, is an allowance and refusal

action. The missing refusal action of claim 1 of the instant application is stated on dependent claim 19 of instant application. Regarding secure lockbox of decrypting/encrypting content is also described throughout the disclosure as being using a cryptography method to encrypt and lock contents. Examiner applies, Stefik US 5,715,403 col. and col. 9 lines 58-60and col. 51 lines 24-31, for the well-known method of cryptography. It would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of locking/encrypting method to secure and protect transmission of contents.

Claims 1-23 of the instant application are envisioned by copending Application No. '666 claims 1-16 in that claims 1-16 of the copending application contain all the limitations of claims 1-23 of the instant application. Claims 1-23 of the instant application therefore are not patently distinct from the copending application claims and as such are unpatentable for obvious-type double patenting.

Claim Rejections - 35 USC § 112

3. Claim 7 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claims are objected to because they include number (See MPEP § 608.01(m)).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Olik Pub. No.: US 2002/0023207 A1 in view of Stefik 5,715,403.

Regarding claims 1 and 12, Olik discloses a method/ computing device of delivering content from a source to a sink by way of a computing device, the method comprising:

an application on the computing device calling to a media base on the computing device with a definition of the content, the source, and the sink (0014-0015; *back-end server (media base)...web-content (content)...web-server of a client-access system (SOTA of source)...client server (sink)*);

a media base providing a protected environment in the computing device and including a common infrastructure of core components effectuating processing of content from any particular source and delivering the processed content to any particular sink (claim 1), and whereby the media base allows content to flow through the computing device in a protected fashion, and allows for arbitrary processing of the protected content in the computing device (0018-0019);

the media base establishing a protected media path based on the defined content, source, and sink to effectuate such delivery, the established protected media path (0018-0019) including:

the media base (fig. 1 element 20);

a source trust authority (SOTA) associated with and corresponding to the source, the SOTA acting as a secure lockbox connecting the source to the media base and representing the source in the protected media path (0017-0019; *web-server of the router transfers web-content to back-end server without seeing any data)*; and

a sink trust authority (SITA) associated with and corresponding to the sink (fig. 1 element 10, and 0009-0010);

the SOTA on behalf of the source establishing trust with respect to the protected media path (0015; *web-server of the router... back-end server... sending service request,... modifying request ... incorporating value reference and authentication token*);

the SOTA determining a particular type of action to be taken with the content as delivered through the protected media path (0014-0017; *determining to act on delivering the web-content to the client*);

the SOTA deciding whether the particular type of action can be taken with the content as delivered through the protected media path and informing the media base regarding same (0014-0017, 0027, and claim 4; *web-server of the router deciding ... should web-content be delivered to client... is client authentic*);

the media base informing the application whether the particular type of action can be taken, and if so the application proceeding by commanding the media base to perform such type of action (0018; *web-server of the router informing back-end server to act on sending web content to authenticated user*).

Olik fails to explicitly disclose the policy being rules and requirements for copying/playing the content and secure lackbox being encryption technique.

However Stefik discloses:

also including a policy engine enforcing policy on behalf of each source, the policy corresponding to the content from the source and including rules and requirements for accessing and rendering the content (col. 17 lines 66-col. 19 lines 21);

decrypting the content from the source if necessary, and translating policy associated with the content from a native format into a format amenable to the policy engine if necessary (col. 38 lines 46-56);

the SITA acting as a secure lockbox connecting the sink to the media base and representing the sink in the protected media path (col. 42 lines 43-60, col. 13 lines 50-col. 14 lines 36, and col. 29 lines 7-8), encrypting content to be delivered to the sink if necessary (col. 51 lines 24-31 and col. 9 lines 45-60), and translating the policy associated with the content from the format of the policy engine into a format amenable to the sink if necessary (col. 17 lines 66-col. 19 lines 21), whereby the sink receives the content and corresponding policy, decrypts the received content if necessary, and renders same based on the received policy (col. 42 lines 43-60, col. 13 lines 50-col. 14 lines 36, and col. 29 lines 7-8); and

the SOTA upon trust being established with respect to the protected media path propagating policy corresponding to the content to be delivered to the protected media path (col. 7 lines 52-col. 8 lines 9 and col. 26 lines 39-col. 27 lines 10).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Stefik within the system of Olik because it is analogues in secure transmission of contents to requesters (abstract). One would have been motivated to do so because it would allow to control contents based on usages as it is well known

at the time of the invention and secure transmission of contents by encrypting/locking contents exchanged between servers and client devices.

Regarding claim 2, Olik further discloses the computing device wherein the media base of the instantiated protected media path further includes at least one supplemental component providing additional protected functionality to the computing device (0015-0018).

Regarding claim 3, Olik further discloses the computing device further having instantiated thereon a media application selecting the content to be delivered, selecting each source for providing the content by way of the protected media path, if necessary selecting each sink to receive the provided content by way of the protected media path, actuating the media base to arrange the protected media path according to each selected source and each selected sink (claims 1-2).

Regarding claim 4, Olik further discloses the computing device wherein the media application provides delivery commands to the media base to control delivery of the content from each selected source to each selected sink (0018).

Regarding claim 5, Stefik further discloses the computing device wherein the media base prevents the media application from having access to the content delivered within the protected media path (col. 26 lines 28-col. 27 lines 10, and col. 7 lines 52-col. 8 lines 9). The rational for combining are the same as claim 1 above.

Regarding claim 6, Olik further discloses the computing device wherein the media base prevents the media application from taking any action with respect to the content contrary to the policy corresponding to the content (col. 26 lines 28-col. 27 lines 10, and col. 7 lines 52-col. 8 lines 9). The rational for combining are the same as claim 1 above.

Regarding claim 7, Olik and Stefik further teach the computing device wherein each SOTA of the instantiated protected media path allows content thereof to be delivered through the protected media path 39 only if the SOTA is satisfied that the media base, the policy engine thereof, each employed component thereof, and each SITA of the protected media path is trustworthy and has rights to be in contact with the content based on the policy corresponding thereto (Olik claim 12 and 0016-0018, and Stefik claim 25). The rational for combining are the same as claim 1 above.

Regarding claim 8, Olik.the computing device wherein any element can be shown to be trustworthy based on a proffer of an acceptable token that vouches for the element (0022).

Regarding claim 9, Olik further discloses the computing device wherein any element can be shown to be trustworthy based on a proffer of a verifiable digital certificate from an acceptable vouching authority (0014).

Regarding claim 10, Olik further discloses the computing device wherein a trustworthy element is trusted to decide whether same can be in contact with the content based on the policy

corresponding thereto and based on whether same can honor the policy corresponding to the content (col. 17 lines 66-col. 19 lines 21).

Regarding claim 11, Stefik further discloses the computing device wherein a trustworthy element is trusted to respond truthfully to a rights-based query from another element (col. 31 lines 54-67).

Regarding claim 13, Olik further discloses the method wherein the media base establishing the protected media path comprises the media base selecting core components thereof that are to handle and operate on the content while being delivered through the protected media path, the core components providing core functionality to the media base (0015-0018).

Regarding claim 14, Olik further discloses the method wherein the media base establishing the protected media path further comprises the media base selecting supplemental components thereof that are to handle and operate on the content while being delivered through the protected media path, the supplemental components providing supplemental functionality to the media base (claim 1-2).

Regarding claim 15, Stefik further discloses the method wherein the SOTA establishing trust with respect to the protected media path comprises:

the SOTA establishing trust with a policy engine of the media base (col. 17 lines 66-col. 19 lines 21);

the trusted policy engine establishing trust with every other element of the protected media path including the SITA (col. 17 lines 66-col. 19 lines 21). The rational for combining are the same as claim 1 above.

Regarding claim 16, Olik further discloses the method wherein establishing trust with any element comprises receiving a proffer of an acceptable token that vouches for the element (0022).

Regarding claim 17, Olik further discloses the method wherein establishing trust with any element comprises receiving a proffer of a verifiable digital certificate from an acceptable vouching authority (0014).

Regarding claim 18, Stefik further discloses the method wherein the SOTA propagating policy corresponding to the content to be delivered to the protected media path comprises:

the SOTA propagating policy to a policy engine of the media base (col. 17 lines 66-col. 19 lines 21);

the policy engine as necessary determining that each element of the protected media path including the SITA satisfies the policy (col. 31 lines 49-67). The rational for combining are the same basis as claim 1 above.

Regarding claim 19, Stefik further discloses the method wherein if the policy engine determines

that a particular element of the protected media path does not satisfies the policy, the policy engine performs an action selected from a group consisting of refusing such element access to the content and preventing content from being delivered through the protected media path (col. 31 lines 49-col. 32 lines 45). The rational for combining are the same as claim 1 above.

Regarding claim 20, Stefik further discloses the method wherein the SOTA propagating policy corresponding to the content to be delivered to the protected media path comprises:

the SOTA propagating policy to a policy engine of the media base (col. 17 lines 66-col. 19 lines 21);

the policy engine propagating the policy to the SITA in the protected media path (col. 17 lines 66-col. 19 lines 21); and

the SITA as a trusted element of the protected media path abiding by such policy (col. 42 lines 43-60 and col. 13 lines 50-col. 14 lines 36). The rational for combining are the same as claim 1 above.

Regarding claim 21, Olik further discloses the method comprising the SOTA determining from the SITA the particular type of action to be taken with the content as delivered through the protected media path (0014-0017).

Regarding claim 22, Stefik further discloses the method comprising the SOTA deciding whether the particular type of action can be taken with the content based on the policy corresponding

thereto (col. 17 lines 66-col. 19 lines 21). The rational for combining are the same as claim 1 above.

Regarding claim 23, Stefik further discloses the method further comprising:

the SOTA obtaining the content from the source in an encrypted form, decrypting the encrypted content, and delivering the decrypted content to the media base (col. 38 lines 34-49);

the media base processing the decrypted content as necessary and delivering the processed content to the SIAT (col. 38 lines 34-49); and

the SITA encrypting the processed content and delivering the encrypted processed content to the sink (col. 51 lines 24-31 and col. 9 lines 45-60). The rational for combining are the same as claim 1 above.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US 2005/0071280 A1 and US 2005/0131832 A1: Trusted relationships between servers.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.
April 10, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER
4/12/06